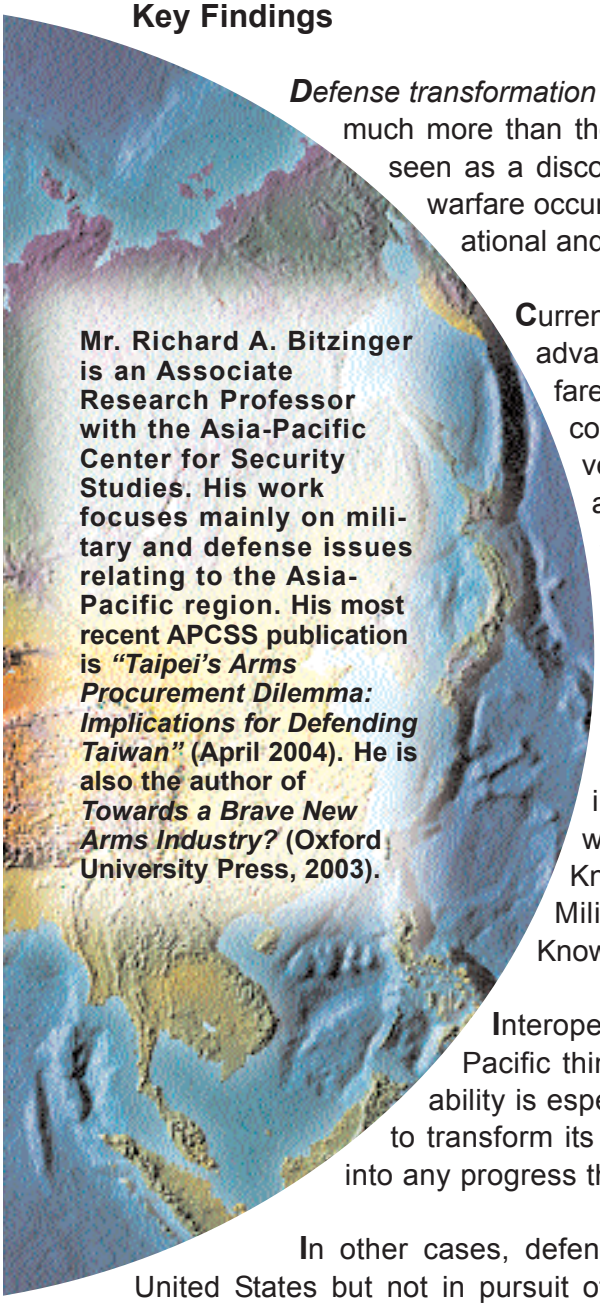
Asia-Pacific Security Studies

Defense Transformation and the Asia Pacific

Implications for Regional Militaries

Asia-Pacific Center for Security Studies Volume 3 - Number 7, October 2004

Key Findings



Mr. Richard A. Bitzinger is an Associate Research Professor with the Asia-Pacific Center for Security Studies. His work focuses mainly on military and defense issues relating to the Asia-Pacific region. His most recent APCSS publication is *"Taipei's Arms Procurement Dilemma: Implications for Defending Taiwan"* (April 2004). He is also the author of *Towards a Brave New Arms Industry?* (Oxford University Press, 2003).

Defense transformation is an ambiguous but nevertheless bounded term. Generally, it is much more than the mere modernization of a country's armed forces; rather, it is seen as a discontinuous or disruptive change in the character and conduct of warfare occurring when new technologies are combined with innovative operational and organizational concepts.

Currently, defense transformation is driven and enabled primarily by advances in information technologies (IT) and network-centric warfare. Key characteristics of a modern transformed force include: new command, control, communications, computing, intelligence, surveillance, and reconnaissance (C4ISR), networked with weapons and platforms; shared situational awareness; more accurate and standoff engagement; agility, speed, rapid deployability, and flexibility; and greater jointness and interoperability.

Militaries and governments throughout the Asia-Pacific region have begun to consider the promise and requirements of defense transformation, including transformational concepts. Most of these typically entail the acquisition, development, and integration of new C4ISR systems and precision-guided weapons. Australia has termed its transformational concept the Knowledge Edge; Japan the Information-based Revolution in Military Affairs (Info-RMA); and Singapore the Integrated Knowledge-based Command and Control (IKC2).

Interoperability with U.S. forces has been a key driver of current Asia-Pacific thinking about defense transformation. This enhanced interoperability is especially crucial for regional allies as the United States continues to transform its armed forces-it would permit these countries' militaries to tap into any progress the United States makes in transformational warfare.

In other cases, defense transformation is driven by considerations related to the United States but not in pursuit of interoperability. For example, China has devoted increased attention to developing capabilities for asymmetric warfare using so-called *assassin's mace* weapons to defeat superior forces. For these reasons, transformation is an increasingly loaded and challenging issue with many implications for defense and security in the Asia-Pacific region.

In recent years, militaries and governments throughout the Asia-Pacific region have begun to pay increasing attention to the promise and requirements of defense transformation and the emerging IT-based revolution in military affairs (RMA). Increasingly, their conception of defense transformation, along with their intentions, efforts, and capabilities to transform their militaries, could have a profound effect upon regional stability and security. These activities could particularly affect future U.S. security interests and military operations in the Asia-Pacific. By endowing new capabilities upon potential competitors and adversaries, defense transformation would inject new uncertainties and complications into the regional security calculus.

The United States is generally recognized to be at the forefront--in terms of strategy, organization, and technology--of conceptualizing and implementing defense transformation. Consequently, U.S. models and paradigms have typically been a critical point of departure for most countries around the world when it comes to the theory and practice of the IT-based RMA and defense transformation. This influence is particularly apparent when one examines the current defense in the Asia-Pacific regarding the potential and requirements for transforming regional militaries.

What is Defense Tranformation?

Defense transformation is an ambiguous but nevertheless bounded term. Many proponents of defense transformation see it as synonymous with the so-called RMA and often view it as a process of implementing the RMA. An RMA is often described as a discontinuous or disruptive change in the concept and mode of warfare. Andrew Krepinevich, a leading analyst and advocate of the RMA, argues that the RMA occurs when:

the application of new technologies into a significant number of military systems combines with innovative operational concepts and organizational adaptation in a way that fundamentally alters the character and conduct of a conflict. It does so by producing a dramatic increase…in the combat potential and military effectiveness of armed forces.

In a similar vein, RAND, a major U.S. military think tank, defines the RMA as:

a paradigm shift in the nature and conduct of military operations which either renders obsolete or irrelevant one or more core competencies in a dominant player, or creates one or more core competencies in some dimension of warfare, or both.

Most analysts and proponents of defense transformation are in general agreement that the current RMA (and therefore the current process of transformation) has been primarily driven and enabled by dramatic advances in IT over the past two or three decades. The information revolution--supplemented by recent advances in new material and construction techniques--have made possible significant innovation and improvement in the fields of sensors, seekers, computing and communications, automation, range, precision, and stealth. In one sense, defense transformation is inexorably linked to emerging concepts of network-centric warfare (NCW), which is sometimes referred to as network-enabled warfare, and vastly improved battlefield knowledge and connectivity due to IT-led breakthroughs in creating more capable C4ISR networks. NCW, according to the U.S. Department of Defense's Office of Defense Transformation:

generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, high tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization.

The key characteristics of a transformed force, therefore, include:

- Networked C4ISR, weapons, and platforms
- Shared situational awareness
- More accurate and standoff engagement
- Agility, speed, rapid deployability, and flexibility
- Jointness and interoperability

In a larger sense, defense transformation is synergistic: It entails the integration and employment of C4ISR systems, platforms, and weapons (particularly "smart" munitions) in ways that increase their effectiveness and capabilities beyond their individual sets. This bundling is reminiscent of Admiral William Owens's systems concept, which links several types of discrete and even disparate systems across a broad geographical, interservice, and electronic spectrum to create new core competencies in war fighting.

Obviously, defense transformation entails much more than mere force modernization. Hardware and technology are obviously crucial and primary components that serve as building blocks in the modern, IT-led RMA centered on NCW and reconnaissance-strike complexes. Transformation, however, is not simply a techno-fix. It fundamentally changes the way the military does business--doctrinally, organizationally, and institutionally. It also requires advanced systems integration skills to knit-together disparate military systems into complex operational networks. Finally, it demands elemental changes in ways the military procures critical equipment and the reform of technological and industrial bases that contribute to the development and production of transformational systems. All this, in turn, requires vision and leadership at the top to develop basic concepts of defense transformation; establish the necessary institutional and political momentum for implementing transformation; and allocate the financial resources and human capital required for implementation.

Recent Developments in Defense Transformation in the Asia-Pacific Region

Several Asia-Pacific militaries have clearly been amassing much of the hardware necessary for defense transformation (See Richard A. Bitzinger, "The Asia-Pacific Arms Market: Emerging Capabilities, Emerging Concerns," Asia-Pacific Security Studies, Asia-Pacific Center for Security Studies, March 2004). The acquisition of new technology, however, is only the first and often the easiest step in realizing an RMA. It is necessary to also develop the software (the doctrines, tactics, and organizations) necessary to take full advantage of these new technologies. Accordingly, many militaries and governments in the Asia-Pacific region have shown increasing attention to studying, assessing, and even experimenting with these software requirements for implementing transformation.

Australia has been looking at the issue of defense transformation since the mid-1990s. In 1999, the Australian Department of Defense established an Office of the Revolution in Military Affairs in order to review technological developments and explore strategies for implementing an Australian RMA, particularly in partnership with the United States. According to one report, the four key components of the Australian RMA are weapons lethality, force projection, information processing, and intelligence collection. As a practical result, Australia stresses developing and enhancing the mobility, firepower, and sustainability of the Australian Defense Forces (ADF) by expanding interservice jointness, increasing logistical support, strengthening amphibious and expeditionary capabilities, and making improve-

ments in precision-strike and intelligence-gathering, surveillance, and reconnaissance (ISR).

In particular, the ADF places increasing emphasis on NCW as a means to gain an edge over potential competitors in the region. The Knowledge Edge concept is defined as the effective exploitation of IT to allow the ADF to use its relatively small force to maximum effectiveness. NCW is intended not only to provide the ADF with a force multiplier to maintain a technological edge over its much larger potential adversaries (such as Indonesia), but also to enhance cooperation and interoperability with U.S. forces. In this regard, Australia seeks to leverage its limited indigenous high-technology core competencies--such as its *Jindalee* over-the-horizon radar network (JORN)--in collaborative weapons programs with the United States.

China has also been particularly influenced by the emerging IT-based RMA. Beijing is currently engaged in a determined effort to modernize its armed forces, the People's Liberation Army (PLA), in order to fight and win limited wars under high-tech conditions. This doctrine revolves around short-duration, high-intensity conflicts characterized by mobility, speed, and long-range attack; employs joint operations fought simultaneously throughout the entire air, land, sea, space, and electromagnetic battle space; and relies heavily upon extremely lethal high-technology weapons. PLA operational doctrine also emphasizes preemption, surprise, and shock value since the earliest stages of conflict may be crucial to the outcome of a war.

In this regard, Beijing sees considerable potential for force multipliers in such areas as information warfare, digitization of the battlefield, and networked systems. As already mentioned, China is greatly expanding its C4ISR capabilities. At the same time, adversaries who are highly dependent upon advanced technology (such as the United States) are seen as susceptible to low-tech countermeasures or attacks on their own command, control, and communications capabilities. Consequently, the PLA has devoted increasing attention to the development of asymmetric responses aimed at enabling "the inferior to defeat the superior." These systems are sometimes lumped together and referred to as assassin's mace or trump card weapons. Some assassin's mace weapons are intended to attack an enemy's vulnerabilities such as computer networks. Information warfare (IW) is a new, potentially critical development in the PLA's war fighting capabilities. The PLA is reportedly experimenting with IW operations, and it has established special IW units to carry out attacks on enemy computer networks in order to blind and disrupt an adversary's command, control, communications, computing, and intelligence (C4I) systems.

India, following the events and outcome of the 1991 Gulf War, began to pay closer attention to the promise and challenges of the emerging IT-based RMA. Many Indians have become increasingly concerned about growing U.S. technological prowess and its near-global dominance as a conventional military power. Consequently, some have called for India to acquire corresponding, perhaps asymmetric capabilities to deal with this new military-technological reality. In particular, this response entails exploiting the emerging information revolution in warfare if India still wants to be taken seriously as a regional and global power, and if it still wants to have a fighting chance in future conflicts. In this regard, India's rapidly growing IT sector is seen as playing a critical role in this effort.

Japan's interest in defense transformation has much of its roots in the 1998 North Korean Taepo Dong missile test, which alerted Tokyo of the need to reform and reorient its Self-Defense Forces (SDF) to new threats, particularly ballistic missiles and the proliferation of weapons of mass destruction (WMD). Other concerns affecting Japan's interest in transformation include the possibility of cyber attacks on its national information infrastructure, the likely expansion of SDF involvement in international military operations (such as in Iraq), and increased military cooperation with the United States in regional security undertakings.

The Japan Defense Agency (JDA) has designated its transformational concept the Info-RMA. The Info-RMA is based on the premise that future warfare will be characterized by a huge leap in battle space awareness capability, precision-strike engagements, coordinated attacks by widely dispersed small units, the heavy use of cyberspace and unmanned battlefield systems, the expansion of the operational theater and increased speed, and the move from attrition to decisive (often called effects-based) warfare. The Info-RMA, according to JDA, is based on the application of advanced IT to the military sphere and entails information-sharing through the creation of an all-inclusive C4ISR network; greater jointness and speed (particularly when it comes to command and control); increased combat efficiency and effectiveness; greater organizational flexibility; the protection of critical information systems (such as command and control nodes); and expanded interoperability with U.S. forces. The objective of this Info-RMA is a quantum leap in the efficient achievement of military objectives.

Many of the principles of the Info-RMA can be found in the SDF's future defense capabilities requirements. In particular, the JDA's 2003 defense posture review calls for the SDF to construct a joint information-sharing network for its ground, sea, and air self-defense forces; shift from a scale-oriented force structure to a technology-oriented force (i.e., use technology as a force multiplier); and maintain interoperability with the United States by catching up with U.S. force modernization and digitization. In addition, Japan plans to greatly increase its missile defense initiatives, such as upgrading its naval Aegis systems to defend against missile attacks and expanding cooperation with the United States on joint missile defense research and development (R&D). In fact, missile defense could become a catalyst for defense transformation in Japan since it could effect critical policy changes (e.g., amending Article 9 of Japan's constitution in order to permit expanded U.S.-Japan cooperation in collective self-defense), promote the acquisition of a joint SDF C4ISR network, and help reform Japan's defense R&D and industrial infrastructure.

Singapore's interest in defense transformation stems both from its strategic weaknesses--lack of strategic depth, a small and aging population, and relatively limited defense resources--and its economic and technological advantages, particularly a highly educated workforce and its IT sector. Singapore's Ministry of Defense (MINDEF) recognizes the criticality of IT as perhaps the most decisive factor in future conflict, as noted in its 2000 defense policy document, *Defending Singapore in the 21st Century*:

[The IT-led RMA will] change the nature of warfare. Superior numbers in platforms…will become less of an advantage unless all these platforms can be integrated into a unified, flexible, and effective fighting system using advanced information technologies. At the same time, the ever-increasing reliance upon information technology means that protecting one's own information systems and disrupting the enemy's will become a major aspect of warfare.

Accordingly, Singapore transformational efforts--the Integrated Knowledge-based Command and Control (IKC2) doctrinal concept--emphasize the acquisition, development, and integration of technologies for command and control with ISR systems and precision-guided weapons. RMA-related areas where MINDEF is currently focusing much of its efforts include advanced electronics and signal processing, information systems security, advanced guidance systems, communications, electronic warfare, sensors, and unmanned vehicles.

To better aid the transformation of Singapore's armed forces

along the lines of the IKC2 concept, MINDEF has established a Future Systems Directorate (FSD) and a Center for Military Experimentation (CME). These two organizations are tasked with helping to implement Singapore's proposed IKC2 concept.

South Korea and Taiwan both appear to be still at the early conceptualization stage of defense transformation. The Republic of Korea (ROK) armed forces are conscious of the fact that future warfare will be quite different from today: nonlinear, small-scale, nonconcentrative, and far-separated. Consequently, future military forces need to develop improved capabilities for C4ISR, including the networking of platforms, unmanned systems, and real-time command and control as well as enhanced capacities for precision-strike. Additionally, the ROK-U.S. alliance is undergoing a shift with South Korea expected to play a larger role in its defense. Seoul is interested in exploring ways to be more self-reliant (particularly when it comes to early warning, intelligence, and surveillance) and still be an interoperable partner with U.S. forces. Nevertheless, it is generally agreed that the Korean RMA is still very much at the starting line.

Taiwan's RMA is largely predicated on Chinese threat scenarios and, therefore, is very much influenced by Chinese thinking about the RMA. Not surprisingly, Taipei is very concerned about defending against a missile strike and securing its command and control network from PLA attacks while also engaging in offensive information warfare against China. Elements of such a doctrine include early warning systems, reconnaissance capabilities, and an integrated and secure command and control system, along with antimissile interceptors and possibly retaliatory ballistic missile systems.

In their efforts to implement an RMA, Seoul and Taipei are aided by the presence of large and growing IT sectors. South Korea and Taiwan are both highly wired in terms of cable and cellular systems, Internet use, and electronics industries. In particular, they possess sizable manufacturing bases in the fields of computers and telecommunications. Together they dominate the global production of dynamic random-access memory (DRAM) semiconductor chips.

Conclusion

Defense transformation has many implications for Asia-Pacific militaries. At the very least, the introduction of new technologies and new armaments promises to significantly affect strategy and operations on tomorrow's battlefield and hence alter the determinants of critical capabilities in modern warfare. Asia-Pacific militaries are clearly acquiring greater lethality and accuracy at greater ranges, improved battlefield knowledge and command and control, and increased operational maneuver and speed. Standoff precision-guided weapons, such as cruise and ballistic missiles and Global Positioning Systems (GPS)-homing guided munitions, have greatly increased combat firepower and effectiveness. The addition of modern submarines and surface combatants, amphibious assault ships, air-refueled combat aircraft, and transport aircraft have extended these militaries' theoretical range of action. Advanced reconnaissance and surveillance platforms have considerably expanded their capacities to look over the horizon and in all three dimensions. Through the increased use of stealth and active defenses (such as missile defense and longer-range air-to-air missiles), local militaries are significantly adding to their survivability and operational capabilities. Consequently, conflict in the region (should it occur) would likely be more high-tech: faster, more long-distance and yet more precise, and perhaps more devastating in its effect.

Defense transformation also has the potential to greatly affect future interoperability between the United States and allied forces in the region. Interoperability has been a key factor driving much of the current thinking about defense transformation in the Asia-Pacific. U.S. allies and friendly partners in the region--Australia, Japan, South Korea, and Taiwan--are considering transformations of their respective militaries in order to remain compatible with U.S. forces, particularly as the likelihood of coalition operations with the United States (such as in Iraq and Afghanistan) is expanding. This enhanced interoperability is especially crucial for regional allies as the United States continues to transform its armed forces; it would permit these countries' militaries to tap into and take advantage of U.S. progress in transformational warfare. For example, Australia, Japan, and South Korea are all acquiring the Aegis combat system, which could enable their ships to link up with U.S. naval forces in cooperative engagements against opposing forces or, as in the case of Australia and Japan, permit it to work with the United States in developing and deploying ship-based missile defenses. At the same time, defense transformation on the part of key U.S. allies and friendly countries in the Asia-Pacific could greatly benefit the United States by strengthening bilateral military alliances and burden-sharing with U.S. forces in the region.

Defense transformation means much more than the mere modernization of a country's armed forces; it is, in fact, the very promise of a paradigm shift in the character and conduct of warfare. For this reason, defense transformation entails more than simply overlaying new technologies and new hardware over existing force structures; rather, it also demands fundamental changes in the ways that future military will organize and fight wars. For these reasons, defense transformation will remain a controversial concept, challenging long-held concepts and cherished shibboleths when it comes to military organization, strategy, and tactics. Subsequently, defense transformation has the potential to greatly impact regional defense and security in the Asia-Pacific.

The Asia-Pacific Center for Security Studies (APCSS) is a regional study, conference, and research center established in Honolulu on September 4, 1995, complementing PACOM's theater security cooperation strategy of maintaining positive security relationships with nations in the region. The APCSS mission is to enhance cooperation and build relationships through mutual understanding and study of comprehensive security issues among military and civilian representatives of the United States and other Asia-Pacific nations.

The Asia-Pacific Security Studies series contributes to the APCSS mission to enhance the region's security discourse. The general editor of the series is Lt. Gen. (Ret.) H.C. Stackpole, President of the APCSS.

Asia-Pacific Center for Security Studies
2058 Maluhia Road Honolulu, Hawaii 96815-1949 (808) 971-8900 fax: (808) 971-8999

www.apcss.org